SD/HDM: CRH
F. #2012R001454/ OCDETF #NYNYE-568

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

– – – – – – – – – – – – – – – – X

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE HEWLETT PACKARD PAVILION LATOP COMPUTER

– – – – – – – – – – – – – – – – X

16M 701

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

No._____

EASTERN DISTRICT OF NEW YORK, SS:

Mark Hadzewycz, being duly sworn, deposes and states that he is a Special Agent with the Drug Enforcement Administration ("DEA"), duly appointed according to law and acting as such.

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—namely, the above-referenced Hewlett Packard Pavilion Laptop Computer, as described in Attachment A—which is currently in law enforcement possession in the Eastern District of New York, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the DEA. I am responsible for investigating narcotics trafficking and money laundering, as well as other offenses. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. During my tenure with the DEA, I have participated in narcotics investigations during the course of which I have: (a) conducted physical and wire surveillance; (b) executed search warrants at locations where drugs, drug proceeds, records of narcotics, money laundering transactions and firearms have been found; (c) reviewed and analyzed numerous taped conversations and records of drug traffickers; (d) debriefed cooperating drug traffickers; (e) monitored wiretapped conversations of drug traffickers and reviewed line sheets prepared by wiretap monitors; and (f) conducted surveillance of individuals engaged in drug trafficking and money laundering. Through my training, education, and experience, I have become familiar with (a) the manner in which illegal drugs are imported and distributed; (b) the method of payment for such drugs; and (c) the efforts of persons involved in such activity to avoid detection by law enforcement.

4. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

IDENTIFICATION OF THE JIMENEZ COMPUTER

5. The property to be searched is as follows: ONE HEWLETT PACKARD PAVILION LAPTOP COMPUTER LABELED DEA EXHIBIT N-116, seized on or about February 26, 2008 from the premises located at 55 Riverwalk Place, Apartment No. 460, West New York, New Jersey (the "JIMENEZ COMPUTER"). The JIMENEZ COMPUTER is in the custody of law enforcement officials in New York, New York.

6. The applied-for warrant would authorize the forensic examination of the JIMENEZ COMPUTER for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. Since 2007, the DEA has been investigating a Mexican-based drug trafficking organization involved in the importation of cocaine, heroin and marijuana into the United States. Based upon this investigation, first, there is probable cause to believe that SALVADOR JIMENEZ URIBE ("JIMENEZ") was engaging in schemes to import cocaine, heroin and marijuana into the United States from Mexico from 2007 until his arrest on or about February 26, 2008,[1] the date that the JIMENEZ COMPUTER was seized by law enforcement officials. Second, there is probable cause to believe that JIMENEZ was using the JIMENEZ COMPUTER to keep ledgers of his narcotics trafficking activity. Third, there is probable cause to believe that JIMENEZ used the JIMENEZ COMPUTER to communicate through emails with drug traffickers to further his drug trafficking activity.

8. On or about February 25, 2008, law enforcement officials conducted surveillance on a blue Toyota Sienna, license plate no. EDE997 (the "BLUE VAN"). Law enforcement officials observed an individual, who later became a cooperating witness for the government ("CW1"), enter the BLUE VAN, along with an unknown male. Law enforcement

[1] JIMENEZ URIBE has been indicted in the Eastern District of New York for International Cocaine Distribution Conspiracy, from May 1, 2012 to March 15, 2015, in violation of Title 21, United States Code, Sections 963, 959(c), and 960(b)(1)(B)(ii), International Narcotics Distribution Conspiracy, from January 1, 2007 to December 31, 2008, in violation of Title 21, United States Code, Sections 963, 959(c), 960(b)(1)(A), 960(b)(1)(B)(ii), and 960(b)(1)(G), Narcotics Distribution Conspiracy, from January 1, 2007 to February 26, 2008, in violation of Title 21, United States Code, Section 846, and Money Laundering Conspiracy, from July 1, 2007 to February 26, 2008, in violation of Title 18, United States Code, Section 1956(h).

officials followed the BLUE VAN through the night. During their surveillance, law enforcement officials observed conduct consistent with drug trafficking activity. Specifically, law enforcement officials observed (i) the BLUE VAN, driven by CW1, pick up an individual for a short period of time and then drop the individual off with a bag in his hand; (ii) the BLUE VAN, driven by CW1, meet up with another individual ("Co-Conspirator-1" or "CC-1") driving a white van (the "WHITE VAN"), travel together to a service station known to law enforcement to be a location often used to conduct narcotics exchanges, enter-and-exit their vehicles, and enter and-exit the service station,; (iii) both the drivers of the BLUE VAN and WHITE VAN engage in maneuvers consistent with counter-surveillance of law enforcement; (iv) CW1 enter-and-exit an apartment located at 55 Riverwalk Place, in West New York, New Jersey (the location of the apartment where the JIMENEZ COMPUTER was found, as described more fully below) while using multiple cellular telephones; and (v) CC-1 leave the WHITE VAN in a parking lot in the Bronx, while the BLUE VAN drove past the WHITE VAN multiple times and periodically park nearby. On or about February 26, 2008, law enforcement officials observed CC-1 drive the BLUE VAN and park the vehicle next to the WHITE VAN in a parking lot near the intersection of Nagle Avenue and Hillside Avenue in the Bronx, New York. Law enforcement officials then observed CC-1 transfer a large black bag from the WHITE VAN to the BLUE VAN. Law enforcement officials then approached CC-1, and observed a white brick-shaped object coming out of a duffle bag located in the BLUE VAN. Law enforcement officials then conducted a search and recovered approximately 114 kilograms of cocaine, 10 kilograms of heroin and a half kilogram of marijuana.

9. Law enforcement officials then arrested CW1 and CC-1. In CW1's possession were keys to the premises located at 55 Riverwalk Place, Apartment No. 460, West

New York, New Jersey (the "RIVERWALK APT"), which was the same location that CW1 visited the prior evening in the BLUE VAN that was found to contain the hundreds of kilograms of narcotics. On or about February 26, 2008, law enforcement officials arrived at the RIVERWALK APT. JIMENEZ answered the door and the law enforcement officials identified themselves. JIMENEZ then provided written consent to search the RIVERWALK APT. During the search, law enforcement officials recovered a black duffle bag and back pack in the bedroom closet that contained U.S. currency tightly packed in bundles in a manner consistent with narcotics trafficking. Law enforcement officials also recovered a money counter, a vacuum sealer, an armored vest, six cellular telephones and the JIMENEZ COMPUTER.

10. CW1 subsequently pled guilty pursuant to a cooperation agreement with the government to narcotics distribution conspiracy, in violation of Title 21, United States Code, Section 846. CW1 stated to law enforcement officials, in sum and substance and in part, that (1) CW1 trafficked approximately 100 kilograms of cocaine every week to ten days from March 2007 to February 2008 with JIMENEZ, selling the cocaine in the New York area; (2) that JIMENEZ and CW1 laundered the narcotics proceeds using a jewelry store operated by a co-conspirator in Queens, New York; and (3) that JIMENEZ communicated with CW1 regarding the narcotics trafficking and money laundering through emails. CWI identified the JIMENEZ COMPUTER as the computer that JIMENEZ used to keep ledgers of their narcotics trafficking activity and money laundering, such as drug shipments, payments, and proceeds amounts. CW1 stated in sum and substance and in part that JIMENEZ and CW1 were in the process of moving handwritten ledgers onto the JIMENEZ COMPUTER and that the JIMENEZ COMPUTER contained such ledgers at the time of the seizure.

11. There is therefore probable cause to believe that the JIMENEZ COMPUTR contains evidence of narcotics trafficking and money laundering, in violation of Title 21, United States Code, Section 846 and Title 18, United States Code, Section 1956(h) respectively.

ITEMS LIKELY TO BE FOUND ON THE JIMENEZ COMPUTER

12. Based on my training, experience and knowledge of the investigation, and experience in searches of electronic devices and computers, there is probable cause to believe that the JIMENEZ COMPUTER contains information related to narcotics trafficking and money laundering, including, but not limited to:

a. Information that discusses the time, location and size of drug shipments ;

b. Information that discusses the payments for the drug shipments;

c. Information regarding the amount of narcotics proceeds and the amounts laundered; and

d. Email communications about narcotics trafficking and money laundering activity;

As described above and in Attachment A and Attachment B, this application seeks permission to search for records that might be found on the JIMENEZ COMPUTER, in whatever form they are found. One form in which the records might be found is data stored on the JIMENEZ COMPUTER's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

60. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe

that this forensic electronic evidence will be on any storage medium in the JIMENEZ COMPUTER because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Lastly, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

61. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, off-site imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Mark Hadzewycz
Special Agent, DEA

Sworn to before me this
27th day

S/ LEVY

THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is ONE HEWLETT PACKARD PAVILION LAPTOP COMPUTER LABELED DEA EXHIBIT N-116, seized on or about February 26, 2008 from the premises located at 55 Riverwalk Place, Apartment No. 460, West New York, New Jersey (the "JIMENEZ COMPUTER")

ATTACHMENT B

1. All records relating to violations of Title 21, United States Code, Section 846 and Title 18, United States Code, Section 1956(h), those violations involving SALVADOR JIMENEZ URIBE and others occurring in and about and between March 2007 and February 2008, including:

a. evidence of who used, owned, or controlled the computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime (or crimes) under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

h. evidence of the times the computer was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the computer;

j. documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;

k. records of or information about Internet Protocol addresses used by the computer;

l. records of or information about the computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

2. Routers, modems, and network equipment used to connect computers to the Internet.

3. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form

(such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

4. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile or cellular telephone, tablets, server computers, and network hardware.

5. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.